REMARKS/ARGUMENTS

The amendments and remarks hereto attend to all outstanding issues in the pending office action of August 18, 2004. Claims 1-16 remain pending in this application. Claims 9 and 15 are amended.

In the Claims

35 U.S.C. §112

Claims 2-7, 9, 15-16 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

With respect to claims 2-7, the step of encoding a program includes the step converting the program to a unitary multiplication. For example, U is a unitary matrix multiplication to which the program may converted to. Therefore, we contend the language of these claims is correct.

With respect to claim 9, Applicant amended the claim to provide proper antecedent basis for this claim.

With respect to claims 15 and 16, Applicant amended claim 15 to correct the typographical error.

We accordingly request reconsideration of the rejections of claims 2-7, 9, 15-16 under 35 U.S.C.§112.

35 U.S.C. §103(a)

The following is a quotation from the MPEP setting forth the three basic criteria that must be met to establish a *prima facie* case of obviousness.

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. MPEP §2142, citing In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Claims 1-3 and 9-16 are rejected under 35 USC 103(a) as being unpatentalbe over a publication to Sander and Tschudin, entitled "Protecting Mobile Agents Against Malicious Hosts" (hereinafter "Sander"), in view of a publication to Staffans, entitled "Quadratic Optimal Control Through Coprime and Spectral Factorizations" (hereinafter "Staffans").

Independent claim 1 is a method for encrypting programs for encrypted execution on a network having a remote host computer, comprising the steps of (with emphasis): encoding a program as a unitary matrix with n rows and n columns, encoding an input data string to the program as a vector of length n, wherein execution of the program on the input data string is realized by matrix multiplication of the unitary matrix with the vector; loading the encoded program and the encoded data string on the host computer; executing the encoded program, using the encoded data string, on the host computer; communicating results from the host computer to the network; and decoding the results into output representative of executing the program with the data string, wherein computations and data associated with the program and data string are unintelligible and useless at the host computer.

Independent claim 15 teaches a secured network for executing encrypted computer programs at a remote host computer without sharing intelligible or otherwise useful program code, computations or data associated with execution, comprising (with emphasis): a control computer for encoding a program as a unitary matrix with n rows and n columns and for encoding an input data string to the program as a vector of length n, wherein execution of the program on the input data string is realized by matrix multiplication of the unitary matrix with the vector. The network further comprises a host computer, in network with the control computer, for loading the encoded program and the encoded data string, the host computer executing the encoded program, using the encoded data string, and communicating results to the control computer for decoding, the host computer having substantially no intelligible or otherwise useful program code, computations or data associated with execution of the program.

On the other hand, Sander in section 3.0 discloses: "Instead of using the more general term 'program' .....we will from now on differentiate between a *function* and the *program* that implements it. Thus, our goal is to *encrypt functions* such that their transformation can again be implemented as a program."

In claims 1 and 15, the program gets encoded or encrypted and not the function, as in Sander.

Furthermore, Sander section 3.2 discloses (with emphasis): "With the requirements of mobile agents in mind we can now state the problem we want to solve: Alice has an algorithm to compute a function *f*. Bob has an input *x* and is willing to compute f(x) for her, but Alice wants Bob to learn nothing substantial about *f*. Moreover, Bob should not need to interact with Alice during computation of *f(x)*. For letting Alice and Bob work together in the way described before, we assume that a function *f* can be encrypted to some other function *E(f)*. The encryption hides the function f and may or may not produce also encrypted output data. We let the notation *P(f)* stand for the program that implements the function f. Alice sends Bob the program *P(E(f))* for the encrypted function *E(f)*. Bob only learns about the program *P(E(f))* that he has to apply to his input *x* and the result of this computation that has to return to Alice".

Thus, sections 3.0 and 3.2 of Sander confirms that function *f* is encrypted - and not the program – which is contrary to claims 1 and 15.

Further, in section 3.2, paragraph one, Sander recites that an input x is stored on the host computer Bob and then Bob applies input *x* to Alice's program *P(E(f))* for calculations.

On the other hand, in claims 1 and 15, data is not stored on the host computer; instead the encoded program and encoded data string load on the host computer from somewhere else for calculations.

And, in section 3.2, paragraph two, Sander recites that Bob applies *P(E(f))* to his input *x* for computation; Sander's input x is raw data. In claims 1 and 15, on the other hand (emphasis added), an input data string is encoded to the program as a vector of length n, where in Sander the input x is left alone and unencrypted.

Finally, in section 3.3, Sander discloses another example where Alice wants to evaluate the function at the Bob's input *x* on Bob's computer is a linear map A. She does not want to reveal A to Bob, so picks at random invertible matrix S and computes $B{:}=SA = E(A)$. She sends *B* to Bob, Bob computes $y{:}=Bx$ and sends *y* back to Alice. Alice computes $S^{-1}y$ and obtains the Ax without having disclosed *A* to Bob.

In Sander, therefore, the function gets encrypted and not the program – which is contrary to both claims 1 and 15. Further, in Sander section 3.3, the input x is stored on the host computer Bob; but, in claims 1 and 15, the encoded input data string loads to host computer from somewhere else. Finally, in Sander section 3.3, only function A gets encrypted as a linear map A and the input data x remains raw (not encrypted); but, in claims 1 and 15, the input data string encodes to the program as a vector of length n.

Note, further, that Sander in paragraph of 3.4 writes (with insert in *italics*): "At this current stage we have to leave it open whether the CEF (*computing the encrypted function*) approach is applicable to arbitrary functions - we even can not claim to have achieved a complete solution for the case of all polynomials." Sander thus admits that it only know how to do CEF for some very special cases; it also clearly articulates that Sander does not disclose a general solution because it presents only a means for encrypting very specific functions, not general programs as in the inventions of claims 1,15, which apply to any computation.

The elements of claims 1 and 15 are also not taught or suggested by Steffans, which discloses quadratic optimal control in cost minimizations. Steffans is not analogous art to claims 1, 15, nor to Sander. Steffans is cited by the Examiner, it appears, because of its citation of matrices. However, Steffans does not teach the elements of claims 1, 15; and, as argued above, neither does Sander.

Based on the above arguments, independent claims 1 and 15 are patentably distinct over Sander and Steffans. Reconsideration is thus requested.

Dependent claims 2-14 and 16 are based on the independent claims 1 and 15, respectively, and benefit from like arguments. However, these claims have additional reasons for patentability. For example, in claim 2, the step of converting the program comprises converting the program by a unitary step multiplication. Sander and Staffans do not teach or suggest converting a program, such as argued above. In claim 3, the step of converting the program comprises converting the program by a unitary matrix multiplication U such that $U \in U_n$ for some integer n, where U_n represents a group of unitary matrices of size n. Again, Sander and Staffans do not teach or suggest similar steps of converting a program.

We accordingly request reconsideration of dependent claims 2-14, and 16.

CONCLUSION

Claims 1-16 are pending in this application. In view of the amendments to the claims and the above remarks, Applicant respectfully requests allowance of the pending claims.

Applicant submits fee with the two months extension under 37 C.F.R. §1.136(a). If any fee is deemed necessary in connection with this Amendment and Response, please charge Deposit Account No. 12–0600.

Respectfully submitted,

LATHROP & GAGE L.C.

Date: 18 JAN 2005

By: ______________________

Curtis A. Vock, Reg. No. 38,356
Lathrop & Gage L.C.
4845 Pearl East Circle
Suite 300
Boulder, CO 80301
Tele: (720) 931-3011
Fax: (720) 931-3001